UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/601,374	06/23/2003	David John Craft	AUS920030401US1	7981

45327 7590 10/23/2008

IBM CORPORATION (CS)
C/O CARR LLP
670 FOUNDERS SQUARE
900 JACKSON STREET
DALLAS, TX 75202

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/601,374	CRAFT ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *22-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *22-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to application amendments filed on 6-18-2008.

2. Claims **22 - 37** are pending. Claims **1 - 21** have been canceled. Claims **22, 31** are independent. This application was filed on **6-23-2003**.

Response to Arguments

3. Applicant's arguments filed 6/18/2008 have been fully considered but they were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose "in response to a LOAD command received from the MPU, the APU is configured... to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU". (see Remarks Page 6)

The Ellison prior art discloses that an instruction or command such as a LOAD command is used. The Ellison prior art does not specifically disclose the LOAD command but the prior art discloses that a command is used to invoke the isolated execution state. (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller; col. 4, lines 63-65; col. 3, lines 43-49: isolated mode instruction is executed; verifies and loads code (software))

The Smeets prior art specifically discloses a MPU and an APU, the secure (APU) and insecure (MPU) processors. (see Smeets col. 2, lines 19-23: one processor secure mode; and one processor insecure mode)

And, the Ellison prior art discloses the isolated region is only accessible by the secure processor. (see Ellison col. 6, lines 15-18: access to the isolated area is restricted)

3.2 Applicant argues that the referenced prior art does not disclose that the "isolated area is established in response to invoking of the isolated execution mode". (see Remarks Page 7)

The Ellison prior art discloses that the isolated region is configured (established) by the execution of the instruction to invoke the isolated operational state. (see Ellison col. 4, lines 63-65; col. 3, lines 43-49: isolated mode instruction is executed; verifies and loads (configures) code or software for isolated operation)

3.3 Applicant argues that the referenced prior art does not disclose, "isolated section accessible only by the APU". (see Remarks Page 8)

The Smeets prior art discloses the situation where one processor is operational in a secure mode and a second processor is operational in an insecure mode at the same time. (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode) And, the Ellison prior art discloses that the isolated region is only accessible by the secure processor. (see Ellison col. 6, lines 15-18: access to the isolated area is restricted)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim **22 - 27, 29 - 36** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Ellison et al.** (US Patent No. **7,082,615**) in view of **Smeets et al.** (US Patent No. **6,769,062**).

Regarding Claim 22, Ellison discloses a secure processing system, comprising:

a) a main processor unit (MPU) coupled to a processor bus; (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller)

b) an attached processor complex (APC) coupled to the processor bus and comprising: a local store configured to store computer instructions and data; (see Ellison col. 4, lines 63-65; col. 3, lines 45-47: load code and data (software), local store)

c) an attached processor unit (APU) coupled to the local store; wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key (see Ellison col. 4, lines 63-65: APU coupled to host (processor) bus; col. 6, lines 38-42: cryptographic key storage), and to operate in a non-isolated state and an isolated state; (see Ellison col. 4, lines 16-22:

partitioned memory, isolated and non-isolated) and

Ellison discloses wherein in response to a LOAD command received from the MPU (see Ellison col. 3, lines 43-45: privileged instruction (such as load command) received and processed by processor), the APC is configured to transition from the non-isolated state to the isolated state (see Ellison col. 4, lines 16-22: based on privileged instruction: partitioned memory, isolated and non-isolated), to transfer a set of computer instructions or data into the isolated section of the local store (see Ellison col. 3, lines 21-25; col. 3, lines 45-49: load code and data to isolated region), and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image)

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partition into isolated and non-isolated sections) Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU. However, Smeets discloses:

d) wherein a general access section accessible by the MPU and an isolated section accessible only by the APU. (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines

18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50: *" … To ensure the integrity of commercial transactions and to prevent fraud, it is necessary for users to keep their private keys secret. Anyone who has access to the private key of a user can masquerade as that user with complete anonymity. Thus, widespread use of digital signatures for electronic commerce and other applications will require technology for secure storage of private keys. … "*)

Regarding Claim 23, Ellison discloses the secure processing system as recited in claim 22, wherein secure processing is performed within the isolated section of the local store of the APC. (see Ellison col. 4, line 63 - col. 5, line 5: secure processing within isolated section, non-secure processing outside)

Regarding Claim 24, Ellison discloses the secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is not accessible by

the MPU. (see Ellison col. 6, lines 13-18: access restricted to isolated region)

Regarding Claim 25, Ellison discloses the secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is unique to the secure processing system. (see Ellison col. 6, lines 64-66: unique cryptographic key (for platform) stored)

Regarding Claim 26, Ellison discloses the secure processing system as recited in claim 22, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store. (see Ellison col. 6, lines 13-15: isolated addressing section only setup and defined when in isolated state)

Regarding Claim 27, Ellison discloses the secure processing system as recited in claim 22, wherein when the APC is operating in the isolated state, the APC is configured to respond to an EXIT command received from the MPU by clearing the isolated section of the local store and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store. (see Ellison col. 5, lines 5-10; col. 3, lines 43-49: privileged instruction (configuration commands), initialize or reset isolated region)

Regarding Claim 29, Ellison discloses the secure processing system as recited in claim 22, wherein the APC further comprises a bus interface unit (BIU) coupled to the

processor bus, and wherein local store and the APU are coupled to the BIU. (see Ellison col. 4, lines 40-45: MCH (bus interface unit) coupled to host (processor) bus)

Regarding Claim 30, Ellison discloses the secure processing system as recited in claim 29, wherein the BIU comprises a load/exit state machine (LSEM) configured to store the cryptographic master key. (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code and data to isolated region, state machine; col. 6, lines 38-42: store cryptographic key)

Regarding Claim 31, Ellison discloses a method for carrying out secure processing, comprising:

a) providing a main processor unit (MPU), a processor bus, (see Ellison Figure 1C: host (processor) bus; col. 4, lines 40-45: interface between processors and memory, I/O controller) and

b) an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store; (see Ellison col. 4, lines 63-65: attached processor (APU), isolated execution)

d) configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required; (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: partitioning isolated region, initiation or configuration command)

e) coupling the MPU to the processor bus; (see Ellison Figure 1C: host (processor)

bus; col. 4, lines 40-45: interface between processors and memory, I/O controller)

f) configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; (see Ellison col. 5, lines 5-10; col. 4, lines 16-22: setup isolated and non-isolated states; col. 6, lines 38-42: store cryptographic key)

g) configuring the APC to respond to a received LOAD command by: transitioning from the non-isolated state to the isolated state; (see Ellison col. 5, lines 5-10: configure and setup (APU, LOAD command) isolated state)

i) transferring a set of computer instructions or data into the isolated section of the local store; (see Ellison col. 7, lines 41-43: software to implement; col. 3, lines 21-25; col. 3, lines 45-47: load code or data into isolated region)

j) using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) and

k) coupling the APC to the processor bus. (see Ellison col. 5, lines 43-46: processor (APC) coupled to memory)

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partition into isolated and non-isolated sections) Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU.

However, Smeets discloses:

h) wherein a general access section accessible by the MPU and an isolated section accessible only by the APU; (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50)

Regarding Claim 32, Ellison discloses the method as recited in claim 31, wherein the secure processing is carried out within the isolated section of the local store of the APC. (see Ellison col. 4, line 63 - col. 5, line 5: secure processing within isolated section)

Regarding Claim 33, Ellison discloses the method as recited in claim 31, wherein the cryptographic master key stored in the APC is not accessible by the MPU. (see Ellison col. 6, lines 13-18: access restricted to isolated region)

Regarding Claim 34, Ellison discloses the method as recited in claim 31, wherein the coupling of the MPU and the APC to the processor bus forms a processing system, and wherein cryptographic master key stored in the APC is unique to the processing system. (see Ellison col. 6, lines 64-66: unique cryptography key (for platform) stored)

Regarding Claim 35, Ellison discloses the method as recited in claim 31, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store. (see Ellison col. 6, lines 13-15: isolated section only exists when setup and executing)

Regarding Claim 36, Ellison discloses the method as recited in claim 31, further comprising: configuring the APC to respond to a received EXIT command when operating in the isolated state by: clearing the isolated section of the local store; and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store. (see Ellison col. 3, lines 43-45; col. 5, lines 5-10: command (i.e. instruction) processing, initiate/exit isolated mode; col. 6, lines 13-15: isolated section only exists when setup and executing)

6. Claims **28, 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ellison-Smeets** and further in view of **Worley, JR et al.** (US PGPUB No. **20020194389**).

Regarding Claim 28, Ellison discloses the secure processing system as recited in claim 22, wherein the APC is configured to use the other cryptographic key to decrypt another set of computer instructions or data. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) Ellison does not specifically disclose whereby to authenticate another set of computer instructions or data. However, Worley discloses wherein configured to authenticate another set of computer instructions or data. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code (instructions or data))

It would have been obvious to one of ordinary skill in the art to modify Ellison-Smeets to enable the capability to authenticate another set of computer instructions or data as taught by Worley. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21: *" … provide a set of secure-platform management services for operational control of hardware resources that neither expose privileged instructions and privileged registers of the hardware nor simulate privileged instructions and privileged registers. … "*)

Regarding Claim 37, Ellison discloses the method as recited in claim 31, wherein the configuring the APC to respond to a received LOAD command comprises: configuring the APC to respond to a received LOAD command by:

a) transitioning from the non-isolated state to the isolated state; (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: command processing, isolated region)

c) transferring a set of computer instructions or data into the isolated section of the local store; (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code or data into isolated region)

d) using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic; (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) and

Ellison discloses wherein to partition the local store into a general access section and an isolated section. (see Ellison col. 4, lines 16-22: partitioning memory, isolated and non-isolated regions) Ellison does not specifically disclose a general access section accessible by the MPU and an isolated section accessible only by the APU.

However, Smeets discloses:

b) a general access section accessible by the MPU and an isolated section accessible only by the APU; (see Smeets Figure 1 (18: insecure processor); (20: security module); Figure 2 (30: secure processor); col. 2, lines 2-5; col. 2, lines 19-23: one processor secure mode; one processor insecure mode; col. 3, lines 18-20; col. 3, lines 26-28: not a secure processor (main processor); col. 3, lines 58-60: secure processor)

It would have been obvious to one of ordinary skill in the art to modify Ellison to

enable the capability for a general access section accessible by the MPU and an isolated section accessible only by the APU as taught by Smeets. One of ordinary skill in the art would have been motivated to employ the teachings of Smeets in order to enable the capability to ensure security based on the widespread usage of digital signatures for electronic commerce and other applications requiring technology for the secure storage of private keys. (see Smeets col. 1, lines 44-50)

Ellison-Smeets discloses wherein using the other cryptographic key to authenticate or decrypt another set of computer instructions or data. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) Ellison does not specifically disclose whereby to authenticate another set of computer instructions or data.

However, Worley discloses:

e) to authenticate another set of computer instructions or data. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code (instructions or data))

It would have been obvious to one of ordinary skill in the art to modify Ellison-Smeets to enable the capability to authenticate another set of computer instructions or data as taught by Worley. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
October 1, 2008